Attorney Docket No. 1466.1084

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Kousetsu SAI

Application No.: Group Art Unit:

Filed: January 26, 2004 Examiner:

For: SECURITY SYSTEM, INFORMATION MANAGEMENT SYSTEM, ENCRYPTION SUPPORT SYSTEM, AND COMPUTER PROGRAM PRODUCT

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-51842

Filed: February 27, 2003

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 26, 2004 By: _____

H.J. Staas
Registration No. 22,010

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 ２月２７日

出 願 番 号
Application Number: 特願２００３－０５１８４２

[ST. 10/C]: [ＪＰ２００３－０５１８４２]

出 願 人
Applicant(s): 富士通株式会社

２００３年１０月１０日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０８３９０１

【書類名】　特許願
【整理番号】　0295715
【提出日】　平成15年 2月27日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 15/00
【発明の名称】　セキュリティシステム、情報管理システム、暗号化支援システム、およびコンピュータプログラム
【請求項の数】　5
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　崔　浩哲
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100086933
【弁理士】
【氏名又は名称】　久保　幸雄
【電話番号】　06-6304-1590
【手数料の表示】
【予納台帳番号】　010995
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9704487
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティシステム、情報管理システム、暗号化支援システム、およびコンピュータプログラム

【特許請求の範囲】

【請求項１】

情報を管理する情報管理システムと、前記情報管理システムにおいて情報の暗号化を行うための支援を行う暗号化支援システムと、を有し、

前記暗号化支援システムには、

情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示す規則情報を記憶する暗号化規則記憶手段と、

前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する暗号化用データ送信手段と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理情報受信手段と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、

前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、が設けられ、

前記情報管理システムには、

前記暗号化用データを前記暗号化支援システムより受信する暗号化用データ受信手段と、

当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、

当該情報管理システムが管理する情報の暗号化を、前記暗号化データ受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、

前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、

前記暗号化手段によって行われた暗号化についての前記処理情報を前記暗号化支援システムに送信する処理情報送信手段と、が設けられ、

てなることを特徴とするセキュリティシステム。

【請求項２】

前記規則情報は、前記規則として、暗号化を行う際に用いる暗号方式と当該暗号化の際に使用する暗号鍵の有効期限とを示し、

前記情報管理システムが情報に暗号化を施した時から現在までの時間が当該情報の区分に対応する前記秘密レベルの前記規則に係る前記有効期限を超えた場合に、

前記警告手段は、当該情報管理システムに対して前記警告を与え、

前記規則情報に示される前記暗号方式が変更された場合に、

前記暗号化用データ送信手段は、当該変更された暗号方式による暗号化を行うための前記暗号化用データを前記情報管理システムに送信し、

前記警告手段は、前記警告として、当該変更された暗号方式に従って情報の暗号化を行うべき旨の警告を与える、

請求項１記載のセキュリティシステム。

【請求項３】

暗号化支援システムが提供する、情報の暗号化を行うための支援を受けることによって、情報を管理する情報管理システムであって、

情報を秘密にしたいレベルである秘密レベルごとに定められた、情報の暗号化の規則を示す規則情報と、当該規則に従って情報の暗号化を行うために必要なデータである暗号化用データとを、前記暗号化支援システムより受信する受信手段と、

当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、

当該情報管理システムが管理する情報の暗号化を、前記受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、

前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、

前記規則に従って情報の暗号化が行われたか否かのチェックを受けるために、前記暗号化手段によって行われた暗号化の処理の内容を示す処理情報を前記暗号化支援システムに送信する処理情報送信手段と、

が設けられてなることを特徴とする情報管理システム。

【請求項４】

情報を管理する情報管理システムに対して情報の暗号化を行うための支援を行う暗号化支援システムであって、

情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示す規則情報を記憶する暗号化規則記憶手段と、

前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する送信手段と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する受信手段と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、

前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、

が設けられてなることを特徴とする暗号化支援システム。

【請求項５】

情報を管理する情報管理システムに対して情報の暗号化を行うための支援を行うコンピュータに用いられるコンピュータプログラムであって、

情報を秘密にしたいレベルである秘密レベルごとの、情報の暗号化の規則を示す規則情報と当該規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する処理と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われている

か否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う処理と、

前記監視によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える処理と、

をコンピュータに実行させるためのコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、機密情報の暗号化管理を行うためのシステムに関する。

【０００２】

【従来の技術】

従来より、企業、学校、政府、または自治体などの機関のために、その機関で取り扱われる情報が漏洩しないようにする様々な対策が提案されている。例えば、これらの機関の内部のネットワークと外部のネットワーク（インターネットなど）との間にファイアウォールを設け、外部から内部へのアクセスを制限しまたは禁止する方法が提案されている。

【０００３】

ところが、ファイアウォールを設けたとしても、内部のネットワークにセキュリティホールがあると、外部からの攻撃を受け、情報が漏洩してしまうおそれがある。その機関に属するユーザ（職員）が、操作を誤って情報を漏洩してしまう可能性もある。また、職員が不正に情報を漏らしてしまう可能性もないとは言えない。また、改ざんや偽造により、情報の内容そのものの正当性が侵される可能性がある。

【０００４】

そこで、暗号化しまたは電子署名を付して情報のデータを取り扱う方法が提案されている。これにより、たとえデータが外部に流出したとしても、暗号を解くことができなければ、その情報の内容を確認することができない。よって、実質的に情報の漏洩を防止することができる。

【０００５】

【発明が解決しようとする課題】

しかし、例えば、複数の支店、営業所、または出張所などの部門を有する大規模な機関において上記の方法を採用するとなると、技術情報（例えば、使用している暗号方式の脆弱性および最新の暗号方式などに関する情報）をチェックすることができかつその技術情報に基づいてセキュリティ対策（セキュリティポリシー）を実行することができる専門の技術者を管理者として部門ごとに配属しなければならない。また、すべての管理者の技術レベルを一定以上に保つ必要がある。そうすると、人件費などのコストが増大してしまう。

【０００６】

そこで、システムセンターなどにおいて各部門で取り扱う情報を一元管理する方法が考えられる。しかし、そうすると、システムセンターと各部門との通信量が増大し、システムセンターにおける処理の負荷が増大し、また、不正に暗号が解かれた場合のリスクが大きくなる、といった問題点が生じる。

【０００７】

このような事情により、大規模な機関において上記の暗号化の方法の活用が上手く図れていないことが多い。

一方、小規模な機関（例えば、ＳＯＨＯなど）においても、上記の暗号化の方法の活用が進んでいないことが多い。暗号化に関する技術情報を得ることやセキュリティ対策を行うことは難しく、実際にこれらの作業を行っても、取り扱う情報の量が少ないと割に合わないからである。

【０００８】

そこで、情報管理を外部の業者に委託（アウトソーシング）することが考えられる。しかし、その業者から情報が漏洩するおそれがないとは必ずしも言えないので、重要な機密情報は手元に置いて管理したいと思う経営者が多い。

【０００９】

本発明は、上記のような問題点に鑑み、部門ごとに自らの情報を管理しつつ、高水準のセキュリティの維持を容易に図ることを目的とする。

【００１０】

【課題を解決するための手段】

本発明に係るセキュリティシステムは、情報を管理する情報管理システムと、前記情報管理システムにおいて情報の暗号化を行うための支援を行う暗号化支援システムと、を有する。前記暗号化支援システムには、情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示す規則情報を記憶する暗号化規則記憶手段と、前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する暗号化用データ送信手段と、前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理情報受信手段と、前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、を設ける。前記情報管理システムには、前記暗号化用データを前記暗号化支援システムより受信する暗号化用データ受信手段と、当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、当該情報管理システムが管理する情報の暗号化を、前記暗号化データ受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、前記暗号化手段によって行われた暗号化についての前記処理情報を前記暗号化支援システムに送信する処理情報送信手段と、を設ける。

【００１１】

好ましくは、前記規則情報は、前記規則として、暗号化を行う際に用いる暗号方式と当該暗号化の際に使用する暗号鍵の有効期限とを示し、前記情報管理システムが情報に暗号化を施した時から現在までの時間が当該情報の区分に対応する前記秘密レベルの前記規則に係る前記有効期限を超えた場合に、前記警告手段は、当該情報管理システムに対して前記警告を与え、前記規則情報に示される前記暗号方式が変更された場合に、前記暗号化用データ送信手段は、当該変更された

暗号方式による暗号化を行うための前記暗号化用データを前記情報管理システムに送信し、前記警告手段は、前記警告として、当該変更された暗号方式に従って情報の暗号化を行うべき旨の警告を与える。

【００１２】

または、情報に対して電子署名を行うための証明書の有効期限を管理する有効期限管理手段を設け、前記監視手段は、前記証明書の有効期限に基づいて、情報に対して電子署名をやり直す必要があるか否かを監視し、前記警告手段は、電子署名をやり直す必要があると判別された場合に、当該情報を管理する前記情報管理システムに対して電子署名をやり直すべき旨の警告を与える。

【００１３】

または、前記情報管理システムに、当該情報管理システムが管理する情報の区分と当該区分に対応する前記秘密レベルとを示す区分秘密レベル情報を前記暗号化支援システムに送信する区分秘密レベル送信手段を設ける。そして、前記監視手段は、情報管理システムより受信した前記処理情報と前記区分秘密レベル情報とを比較することによって前記監視を行う。

【００１４】

【発明の実施の形態】

図１は本発明に係るセキュリティシステム１の構成の例を示す図、図２は機密情報サーバ３１のハードウェア構成の例を示す図、図３は機密情報サーバ３１の機能的構成の例を示す図、図４はポリシー管理サーバ２１の機能的構成の例を示す図、図５は暗号化ランクテーブルＴＢ４の例を示す図、図６は機密情報グループテーブルＴＢ５の例を示す図、図７は部署メンバーテーブルＴＢ６の例を示す図、図８は署名期限テーブルＴＢ７の例を示す図、図９は作成データ管理テーブルＴＢ０の例を示す図、図１０はシステム管理部門が有する例外属性テーブルＴＢ８の例を示す図、図１１はある営業所Ｍが有する例外属性テーブルＴＢ９の例を示す図、図１２は顧客連絡先テーブルＴＢ１の例を示す図、図１３は検針情報テーブルＴＢ２の例を示す図、図１４は料金支払テーブルＴＢ３の例を示す図、図１５は暗号化および電子署名の処理の手順の例を示す図である。

【００１５】

本発明に係るセキュリティシステム１は、図１に示すように、暗号化支援システム２、機密情報管理システム３、およびネットワーク４などによって構成される。暗号化支援システム２と機密情報管理システム３とは、ネットワーク４を介して互いに接続可能である。ネットワーク４として、イントラネット、インターネット、公衆回線、または専用線などが用いられる。また、暗号化支援システム２と機密情報管理システム３との間には認証が成立していることが望ましい。

【００１６】

このセキュリティシステム１は、例えば、複数の営業所または支店などの部門を有する会社または複数の支所または出張所などの部門を有する行政機関などに設けられる。以下、複数の営業所を有する会社Ｘに設けられたセキュリティシステム１を例に説明する。

【００１７】

機密情報管理システム３は、機密情報サーバ３１および端末装置３２などによって構成される。この機密情報管理システム３は、営業所ごとに設けられており、その営業所の顧客情報、研究中の技術に関する情報、営業活動などのノウハウ、他社についての調査報告、財務情報、および人事情報など、種々の機密情報（社外秘情報）の管理を行う。

【００１８】

これらの機密情報には、暗号化および電子署名の処理が施されている。また、これらの機密情報は、機密情報サーバ３１において、テキストエディタ、ワープロソフト、表計算ソフト、またはグラフィックソフトなどで作成されたテキストファイルまたはバイナリファイルとして管理され、またはデータベースのレコードとして管理される（図１２、図１３、図１４参照）。以下、これらのファイルまたはレコードつまり機密情報のデータを「機密データＳＤＴ」と記載する。

【００１９】

機密情報サーバ３１は、図２に示すように、ＣＰＵ３１ａ、ＲＡＭ３１ｂ、ＲＯＭ３１ｃ、磁気記憶装置３１ｄ、ディスプレイ装置３１ｅ、マウスまたはキーボードなどの入力装置３１ｆ、および各種インタフェースなどによって構成される。磁気記憶装置３１ｄには、オペレーティングシステム（ＯＳ）および後に示

す各機能を実現するためのプログラムおよびデータなどがインストールされている。これらのプログラムおよびデータは、ＣＤ－ＲＯＭなどの記録媒体によって提供されまたはポリシー管理サーバ２１によってネットワーク４を介して提供される。そして、必要に応じてＲＡＭ３１ｂにロードされ、ＣＰＵ３１ａによってプログラムが実行される。

【００２０】

このような構成によって、機密情報サーバ３１には、図３に示すように、ポリシー適用部３０２、暗号化実行部３０３、署名処理実行部３０４、機密情報更新部３０５、グループ情報通知部３０６、アクセスログ通知部３０７、インデックス管理部３０８、メンバー情報通知部３０９、暗号ポリシーデータベース３Ｄ１、機密情報グループデータベース３Ｄ２、例外属性データベース３Ｄ３、メンバーグループデータベース３Ｄ４、機密情報データベース３Ｄ５などの機能が実現される。

【００２１】

端末装置３２は、営業所の各部署に１台または複数台設置されており、その営業所に配属されている社員が機密情報を取り扱うために使用される。ただし、社員ごとに機密情報の使用権限（アクセス権）が設定されている。これについては、後に説明する。

【００２２】

暗号化支援システム２は、ポリシー管理サーバ２１および端末装置２２などによって構成される。この暗号化支援システム２は、会社Ｘのシステムを統括するシステム管理部門などによって管理されている。ポリシー管理サーバ２１は、各営業所の機密情報管理システム３において行われる機密データＳＤＴのセキュリティ管理のための、支援に関する処理を行う。端末装置２２は、システム管理部門の管理者がポリシー管理サーバ２１の操作を行うために用いられる。システム管理部門は、セキュリティを統括して管理する権限を有していればよく、専任であるか兼任であるかは問わない。

【００２３】

ポリシー管理サーバ２１は、図２に示す機密情報サーバ３１と同様のハードウ

ェア構成をしており、図４に示すようなポリシー情報配付部２０２、適用状況監視部２０３、適用状況集計部２０４、適用警告部２０５、脆弱性監視部２０６、例外属性送信部２０７、暗号ポリシーデータベース２Ｄ１、機密情報グループデータベース２Ｄ２、例外属性データベース２Ｄ３、メンバーグループデータベース２Ｄ４、およびアクセスログデータベース２Ｄ５などの機能が実現される。

【００２４】

以下、図３に示す機密情報サーバ３１および図４に示すポリシー管理サーバ２１の各部の機能について、機密データＳＤＴのセキュリティ管理のための機能とそれを実現する準備のための機能とに大別して説明する。

【００２５】

〔セキュリティ管理の準備のための機能〕

会社Ｘでは、自社のセキュリティ方策（セキュリティポリシー）および個人情報保護方策（個人情報保護ポリシー）の一環として暗号ポリシーを定めている。「暗号ポリシー」とは、機密情報のデータ（機密データＳＤＴ）を暗号化する際に守らなければならない規則、取決め、および方策などを意味するものである。会社Ｘは、自社の暗号ポリシーとして、機密情報の重要性または秘密性（秘匿性）などの大きさに応じた幾つかのランク（レベル）を定めている。以下、これを「暗号化ランク」と記載する。そして、この暗号化ランクごとに暗号化のルールを定めている。

【００２６】

例えば、図５に示すように、暗号化ランクＡ、Ｂ、…ごとに、暗号化のルールとして、暗号方式および更新頻度を定めている。「暗号方式」とは、機密データＳＤＴを暗号化する際に用いる暗号技術のことである。例えば、ＤＥＳ（Data Encryption Standard）、３ＤＥＳ、ＦＥＡＬ（Fast Data Encipherment Algorithm）、ＩＤＥＡ（International Data Encryption Algorithm）、またはＲＳＡ（Rivest Shamir Adleman）などの暗号技術が用いられる。「更新頻度」とは、暗号化をやり直す頻度つまり周期を意味する。例えば、「６０日」と定められている場合は、６０日以内ごとに新たな暗号鍵を生成し、その暗号鍵によって暗号化をやり直さなければならない。

【００２７】

なお、本実施形態において、図５の「暗号化ランク」のランク（レベル）は、全体的に見てＡ、Ｂ、…の順に暗号の解読が難しくなる傾向を示しているが、常に暗号の解読の困難性を示すものではない。上に説明したように、本実施形態の暗号化ランクは、「暗号方式」および「更新頻度」などを組み合わせた暗号化のルールを識別するために用いられる。もちろん、他の実施形態として、暗号化ランクを暗号の解読の困難性を示すものとして用いることも可能である。

【００２８】

ポリシー管理サーバ２１（システム管理部門）の管理者は、端末装置２２を操作するなどして、各暗号化ランクの暗号化のルールを入力し、図５に示す暗号化ランクテーブルＴＢ４を作成する。この際に、会社Ｘで取り扱われる各機密情報の機密データＳＤＴをいずれの暗号化ランクのルールに基づいて暗号化すべきであるかを決める。そして、各暗号化ランクに属する機密情報の区分（属性、クラス）の名称を「機密情報」のフィールドに指定する。なお、本実施形態では、機密情報の区分のために、その機密情報の機密データＳＤＴが格納場所であるテーブルまたはディレクトリが用いられる。

【００２９】

図４の暗号ポリシーデータベース２Ｄ１は、作成された暗号化ランクテーブルＴＢ４を記憶し管理する。また、各暗号方式（α、β、…）ごとに、その暗号方式に基づいて暗号化を行うために必要な暗号化用データＤＴ５を記憶する。暗号化用データＤＴ５の形態として、その暗号方式を実行するためのメインプログラムファイルまたはその暗号方式に用いられる関数または数値などのデータファイル（いわゆるライブラリ）などがある。

【００３０】

ポリシー情報配付部２０２は、暗号化ランクテーブルＴＢ４および暗号化用データＤＴ５を各営業所の機密情報サーバ３１に送信することによって、会社Ｘの暗号ポリシーの情報を配付する。暗号化ランクテーブルＴＢ４の内容が更新された場合は、新しい暗号化ランクテーブルＴＢ４を配付する。この場合は、更新された個所（レコード）だけを配付するようにしてもよい。暗号化用データＤＴ５

が更新または追加された場合も、その新たな暗号化用データＤＴ５を各機密情報サーバ３１に配付する。

【００３１】

図３のポリシー適用部３０２は、ポリシー管理サーバ２１から送信されてきた暗号化ランクテーブルＴＢ４を暗号ポリシーデータベース３Ｄ１に記憶させ、暗号化用データＤＴ５を所定のディレクトリに格納する。つまり、機密情報サーバ３１に会社Ｘの暗号ポリシーを適用し、この暗号ポリシーに基づいて暗号化の処理を実行することができるように、プログラムおよびデータのインストールを行う。更新された暗号化用データＤＴ５または暗号化ランクテーブルＴＢ４のレコードが送信されてきた場合は、対応する古い暗号化用データＤＴ５またはレコードと置き換える。

【００３２】

機密情報グループデータベース３Ｄ２は、図６に示すような機密情報グループテーブルＴＢ５を記憶し管理する。サーバＩＤは、機密データＳＤＴが格納されている装置つまり機密情報サーバ３１を識別するためのＩＤである。機密情報グループＧ１、Ｇ２、…は、それぞれ、機密情報サーバ３１で管理される機密データＳＤＴのうちの使用権限の与えられた利用者グループ（部署）が同一でありかつ暗号化ランクが同一である機密データＳＤＴの区分をグループ化したものである。

【００３３】

例えば、機密情報グループテーブルＴＢ５の第一レコード（サーバＩＤ＝Ｓ００１、機密情報グループ＝Ｇ１）によると、営業所Ｍの料金支払テーブルＴＢ３（図１４参照）および検針情報テーブルＴＢ２（図１３参照）に格納される機密情報の機密データＳＤＴが、「暗号化ランク＝Ｃ」に対応する暗号方式によって暗号化され、かつ、第１課（顧客窓口の部署）の社員に対して使用する権利が与えられていることが、分かる。どの機密情報がどの機密情報グループに属するのかは、ポリシー管理サーバ２１から取得した暗号化ランクテーブルＴＢ４（図５参照）に示される暗号ポリシーに従って、営業所ごとに定められる。

【００３４】

なお、暗号化ランクテーブルＴＢ４において、「ランク＝Ｃ」のように１つの暗号化ランクに複数の暗号方式が対応付けられている場合がある。この場合は、その営業所の管理者が機密情報の使用の利便性などに応じていずれか１つの暗号方式を選択し、機密情報グループテーブルＴＢ５に指定すればよい。または、機密情報管理システム３の環境（例えば、機密情報管理システム３のネットワークの設定情報、機密情報サーバ３１のＯＳの堅牢性、またはその機密情報の使用頻度など）に基づいて、いずれかの暗号方式を自動的に選択するように構成してもよい。また、「他社秘密情報」のように暗号化ランクが複数ある機密情報については、その営業所の管理者が、機密情報ごとにその秘匿性または重要性などに応じていずれかの暗号化ランクを選択すればよい。

【００３５】

機密情報グループテーブルＴＢ５の「暗号化ビット数」は、その機密情報グループの暗号方式による暗号化の際に用いられる暗号鍵のサイズを示す。「レコード数」は、その機密情報グループに属する項目（区分）の機密データＳＤＴの総数である。

【００３６】

図３のグループ情報通知部３０６は、上記のように定められた機密情報グループテーブルＴＢ５をポリシー管理サーバ２１に送信することによって、各機密情報の機密データＳＤＴをどのように暗号化するのかをシステム管理部門に通知する。つまり、営業所のローカルの暗号ポリシーを通知する。図４の機密情報グループデータベース２Ｄ２は、各営業所から送信されてきた機密情報グループテーブルＴＢ５を記憶し管理する。

【００３７】

図３のメンバーグループデータベース３Ｄ４は、図７に示す部署メンバーテーブルＴＢ６、図８に示す署名期限テーブルＴＢ７、および図９に示す作成データ管理テーブルＴＢ０（ＴＢ０ａ、ＴＢ０ｂ、…）を記憶し管理する。

【００３８】

部署メンバーテーブルＴＢ６には、機密情報サーバ３１の利用者すなわち営業所の各部署の社員の一覧が格納されている。署名期限テーブルＴＢ７には、その

社員それぞれの電子署名用の署名鍵の有効期限を示す情報が格納されている。作成データ管理テーブルＴＢ０は、社員（メンバー）ごとに１つずつ設けられ、その社員が署名した文書（機密データＳＤＴ）の文書ＩＤを格納する。

【００３９】

メンバー情報通知部３０９は、部署メンバーテーブルＴＢ６、署名期限テーブルＴＢ７、および作成データ管理テーブルＴＢ０をポリシー管理サーバ２１に送信することによって、営業所の社員の情報をシステム管理部門に通知する。図４のメンバーグループデータベース２Ｄ４は、各営業所から送信されてきた部署メンバーテーブルＴＢ６、署名期限テーブルＴＢ７、および作成データ管理テーブルＴＢ０を記憶し管理する。

【００４０】

前に述べたように、機密データＳＤＴの暗号化を行う際のルールは営業所ごとに図６の機密情報グループテーブルＴＢ５によって定められているが、システム管理部門（暗号化支援システム２）は、この暗号化のルールの例外を、図１０に示す例外属性テーブルＴＢ８によって定めることができる。

【００４１】

例えば、図５の暗号化ランクテーブルＴＢ４に示すように、会社Ｘの暗号ポリシーによると、各営業所は、社内人事に関する機密情報の機密データＳＤＴを「暗号化ランク＝Ｂ」と設定しなければならない。そこで、ある営業所（例えば、営業所Ｍ）では、図６に示すように、社内人事情報テーブルに格納される機密データＳＤＴの暗号化ランクを「Ｂ」に設定している。しかし、システム管理部門は、このルールの例外として、図１０の例外属性テーブルＴＢ８のように、営業所Ｍの社内人事情報テーブルについて「暗号化ランク＝Ａ」と設定することができる。また、１つの営業所単位で指定するだけではなく、「全社」の「料金支払テーブル」のように複数の営業所をまとめて指定することも可能である。これにより、複数の営業所に共通する機密情報の区分の暗号化ランクを一時的に一斉に設定することができる。

【００４２】

このような例外の設定は、例えば、次のような場合に行えばよい。例えば、そ

の営業所の機密情報管理システム３の中にセキュリティホールが見つかった場合、その営業所の社員のパスワードまたは暗号鍵が漏洩するなどして特定の機密データＳＤＴへの不正なアクセスの危険性が高まった場合、または実際に不正なアクセスが行われたために特定の営業所または不特定の営業所に対して機密データのセキュリティが保証されない状況が発生したと考えられる場合などである。これにより、効率的にセキュリティを高めることができる。

【００４３】

この例外属性テーブルＴＢ８は、図４の例外属性データベース２Ｄ３によって記憶され管理される。そして、例外を示す各レコードは、例外情報ＤＴ４として、その例外が与えられた営業所に対して例外属性送信部２０７によって送信される。各営業所の例外属性データベース３Ｄ３（図３参照）は、送信されてきた例外情報ＤＴ４を例外属性テーブルＴＢ９に格納し管理する。例えば、営業所Ｍでは、図１１に示すように、受信した例外情報ＤＴ４が格納される。

【００４４】

機密情報データベース３Ｄ５は、機密情報の機密データＳＤＴを、レコードとしてテーブルに格納し管理する。または、ファイルとして磁気記憶装置３１ｄ（図２参照）の所定のディレクトリに格納し管理する。会社Ｘが電力会社である場合は、例えば、図１２に示す顧客連絡先テーブルＴＢ１にはから電力の供給などのサービスを受ける顧客の連絡先を示す機密データＳＤＴが格納され、図１３に示す検針情報テーブルＴＢ２には顧客が使用した電力量（検針値）を示す機密データＳＤＴが格納され、図１４には電気料金の支払方法に関する機密データＳＤＴが格納される。これらの機密データＳＤＴは、次に説明するような暗号化および電子署名の処理が施された上で管理される。

【００４５】

〔セキュリティ管理（暗号化および電子署名）のための機能〕

暗号化実行部３０３および署名処理実行部３０４は、図６に示す機密情報グループテーブルＴＢ５および図１１に示す例外属性テーブルＴＢ９を参照し、それぞれ、機密データＳＤＴの暗号化の処理および電子署名の処理を行う。これらの処理は、例えば、図１５に示すような流れで行われる。

【００４６】

署名処理実行部３０４は、機密データの作成者または承認者などに対応付けられて設定されている署名方式によって電子署名を生成するとともに（＃１）、タイムスタンプ（TST ：Time Stamp Token）を受け取る（＃２）。電子署名の生成は、例えば、ハッシュ関数によって機密データＳＤＴを圧縮し暗号化することによって行う。ハッシュ関数として、ＭＤ５（Message Digest Algorithm 5）、ＳＨＡ－１（Secure Hash Algorithm １）、またはＨＭＡＣ（Hashed Based Message Authentication Code）などが用いられる。

【００４７】

暗号化実行部３０３は、機密情報グループデータベース３Ｄ２に記憶されている図６の機密情報グループテーブルＴＢ５を参照し、電子署名およびＴＳＴが添付された機密データＳＤＴを暗号化する（＃３）。例えば、作成したプログラムのソースファイルを機密データＳＤＴとしてソースファイルディレクトリに格納する場合は、σ暗号方式によって暗号化を行う。

【００４８】

ただし、図１１の例外属性テーブルＴＢ９に暗号化の例外が設定されている機密情報の機密データＳＤＴについては、この例外に示される暗号化ランクの暗号方式によって暗号化を行う。

【００４９】

ステップ＃３で用いられる暗号鍵は、例えば、その営業所または部署ごとにフロッピディスクなどの記録媒体に保存（記録）され管理される。そして、暗号化を行うごとに機密情報サーバ３１にロードして用いられる。また、署名鍵は、機密データＳＤＴを作成しまたは更新した本人のものが用いられ、普段は本人が所持するＩＣカードなどに記録されている。

【００５０】

電子署名およびＴＳＴが添付され暗号化された機密データＳＤＴは、機密情報データベース３Ｄ５によって管理される（＃４）。なお、暗号化および電子署名の処理が完了すると、処理が完了した旨、処理対象、および使用した暗号方式および署名方式などを示す処理完了情報ＤＴ１をポリシー管理サーバ２１に送信す

る。また、機密情報グループテーブルＴＢ５（図６参照）の「レコード数」を修正する。さらに、機密データＳＤＴの作成者の作成データ管理テーブルＴＢ０（図９参照）にその機密データＳＤＴの文書ＩＤを追加する。

【００５１】

図３に戻って、機密情報更新部３０５は、機密情報データベース３Ｄ５で管理されている機密情報の内容つまり機密データＳＤＴを更新するための処理を行う。まず、暗号化されている機密データＳＤＴを復号し、その内容を端末装置３２のディスプレイ装置に表示する。社員による内容の修正の操作を受け付ける。そして、暗号化実行部３０３および署名処理実行部３０４に対して、暗号化および電子署名の処理を行うように指令する。これにより、更新された機密データＳＤＴに対して、図１５に示す処理が再度施される。この機密データＳＤＴは、更新前の機密データＳＤＴと置き換えられる。なお、修正（更新）が行われなかった場合つまり機密情報の閲覧のみ行われた場合は、閲覧が終わった後、復号された機密データＳＤＴは破棄され、元の機密データＳＤＴがそのまま残される。

【００５２】

アクセスログ通知部３０７は、機密データＳＤＴへのアクセスがあったときに、その日時、その機密データＳＤＴの属する機密情報グループ、およびアクセスした社員などに関するログ情報ＬＤＴをポリシー管理サーバ２１に通知する。例えば、機密データＳＤＴの内容が修正（更新）されまたは閲覧されたときに、ログ情報ＬＤＴを通知する。また、アクセスを試みたが失敗した場合も、その旨を示すログ情報ＬＤＴを通知する。

【００５３】

図４のアクセスログデータベース２Ｄ５は、各営業所の機密情報サーバ３１から送信されてきたログ情報ＬＤＴを記憶し管理する。この際に、営業所ごとに識別コードを割り振り、ログ情報ＬＤＴに送信元の営業所の識別コードを対応付けておく。これらのログ情報ＬＤＴは、例えば、機密データＳＤＴへの不正なアクセスがあった場合に犯人などを特定するために用いられる。

【００５４】

図３のインデックス管理部３０８は、機密情報データベース３Ｄ５が管理する

各テーブル（図１２、図１３、図１４参照）および各ディレクトリに格納されている暗号化された機密データＳＤＴに関するインデックスを作成し、管理する。例えば、機密データＳＤＴの格納場所を示すテーブル名またはディレクトリ名、暗号方式、署名方式、作成者または更新者、または作成日または更新日などを示すインデックスを作成し、管理する。

【００５５】

図４の適用状況監視部２０３は、各営業所の機密情報サーバ３１における暗号ポリシーの適用の状況の監視を行う。監視は、営業所の機密情報サーバ３１から送信されてきた処理完了情報ＤＴ１とその営業所の機密情報グループテーブルＴＢ５（図６参照）および例外属性テーブルＴＢ８（図１０参照）とを比較することによって行う。

【００５６】

例えば、機密情報グループテーブルＴＢ５に指定されるすべての機密情報の区分に対応する処理完了情報ＤＴ１が揃い、かつ、これらの処理完了情報ＤＴ１が機密情報グループテーブルＴＢ５に指定される暗号方式および署名方式を示していることが確認できた場合は、暗号ポリシーが正しく適用されていると判別する。所定の期間が経過しても処理完了情報ＤＴ１が揃わない場合または指定される暗号方式または署名方式とは異なる方式で処理が行われたと確認された場合は、暗号ポリシーが正しく適用されていないと判別する。ただし、指定される暗号方式とは異なる方式で処理が行われた場合であっても、例外属性テーブルＴＢ８に示される例外に基づいて処理が行われた場合は、暗号ポリシーが正しく適用されていると判別する。

【００５７】

適用状況集計部２０４は、適用状況監視部２０３による監視の結果を集計し、ディスプレイ装置に表示しまたはレポートとして用紙に印刷し、システム管理部門または各営業所の管理者などに知らせる。

【００５８】

適用警告部２０５は、暗号ポリシーが正しく適用されていないと判別された場合に、その営業所に対して、直ちに暗号ポリシーを正しく適用すべき旨のメッセ

ージを送信することによって警告を行う。

【００５９】

適用状況監視部２０３は、図５の暗号化ランクテーブルＴＢ４に示される暗号化を行う周期（更新頻度）および図８の署名期限テーブルＴＢ７に示される電子署名に使用される証明書（以下、単に「電子署名」と記載する。）の有効期限の監視を行う。そして、前に暗号化を行った時点から「更新頻度」フィールドに示される時間が過ぎた場合は、適用警告部２０５は、対応する機密情報の機密データＳＤＴの暗号化をやり直すべき旨の警告を行う。電子署名の有効期限が過ぎた場合は、対応する機密情報の機密データＳＤＴに新たな電子署名を付すべき旨の警告を行う。なお、これらの周期または期限が来る所定の期間前（例えば１週間前）に予告のメッセージを送信するようにしてもよい。

【００６０】

脆弱性監視部２０６は、ネットワークに関するサービスを提供する機関など（コンピュータメーカ、通信機器メーカ、インターネットサービスプロバイダ、またはセキュリティサービス会社など）から暗号化および電子署名などに関する技術情報を取得し、機密情報管理システム３で用いられている暗号化および電子署名の脆弱性に関する監視を行う。つまり、現在採用している暗号方式などが妥当なものであるか否かの監視を行う。技術情報は、例えば、脆弱性定義ファイルとして提供される。脆弱性の監視は、この脆弱性定義ファイルの内容と図５に示す暗号化ランクテーブルＴＢ４に定義される暗号方式とをマッチングすることによって行う。

【００６１】

脆弱性が発見された場合は、システム管理部門の管理者に対して警告を行う。このとき、管理者は、直ちに脆弱性をなくすための対策を講じる。例えば、各営業所の管理者に対して注意を促す、暗号化レベルを上げる、暗号鍵を交換する、または新たな暗号方式などを採用する、などの対策を講じる。また、ポリシー情報配付部２０２は、必要に応じて、脆弱性を解決するための新たな暗号化用データＤＴ５または暗号化ランクテーブルＴＢ４（図５参照）を各機密情報管理システム３に配付する。

【００６２】

図１６は暗号化および電子署名の処理の流れの例を説明するフローチャート、図１７はシステム管理部門側の準備の処理の流れの例を説明するフローチャート、図１８は営業所側の準備の処理の流れの例を説明するフローチャート、図１９は運用開始後の処理の流れの例を説明するフローチャート、図２０は機密情報へのアクセス要求があった場合の機密情報サーバ３１における処理の流れの例を説明するフローチャート、図２１は各種設定の変更があった場合の機密情報サーバ３１における処理の流れの例を説明するフローチャートである。

【００６３】

次に、ポリシー管理サーバ２１および機密情報サーバ３１における処理の流れを、フローチャートを参照して説明する。各営業所において会社Ｘのセキュリティポリシーに適合した機密情報の管理を実現するために、ポリシー管理サーバ２１および機密情報サーバ３１は、それぞれ、図１６（ａ）および図１６（ｂ）に示すような手順で処理を行う。

【００６４】

ポリシー管理サーバ２１は、各営業所の機密情報の機密データＳＤＴの暗号化および電子署名の支援のための準備を行う（＃１１）。すなわち、図１７に示すように、会社Ｘのセキュリティポリシーに基づいて策定された暗号ポリシーを入力し（＃１１１）、図５に示すような暗号化ランクテーブルＴＢ４を作成する（＃１１２）。また、暗号化および電子署名の処理を行うために必要なメインプログラムおよびライブラリなどのデータ（暗号化用データＤＴ５）を用意する（＃１１３）。そして、これらの暗号化ランクテーブルＴＢ４および暗号化用データＤＴ５を各営業所の機密情報サーバ３１に送信する（＃１１４）。

【００６５】

一方、機密情報サーバ３１は、その営業所の機密データＳＤＴの暗号化および電子署名のための準備を行う（＃２１）。すなわち、図１８に示すように、ポリシー管理サーバ２１から送信されてきた暗号化ランクテーブルＴＢ４および暗号化用データＤＴ５をインストールする（＃２１１）。

【００６６】

機密情報を扱う社員のうち図７に示す部署メンバーテーブルＴＢ６に登録されていない者がいる場合は（＃２１２でＹｅｓ）、その者を部署メンバーテーブルＴＢ６に追加する（＃２１３）。併せて、その者に対して署名鍵を発行し、発行された署名鍵に含まれる有効期限を取得し、図８に示す署名期限テーブルＴＢ７にその署名鍵の有効期限を設定する（＃２１４）。

【００６７】

また、暗号方式、署名方式、およびアクセス権の設定がなされていない機密情報の区分がある場合は（＃２１５でＹｅｓ）、図６に示す機密情報グループテーブルＴＢ５にそれらの設定を行う（＃２１６）。つまり、機密情報グループの設定を行う。

【００６８】

そして、図６、図７、および図８の各テーブルをポリシー管理サーバ２１に送信することによって、その営業所における暗号化のルールおよび社員の情報をシステム管理部門に通知する（＃２１７）。

【００６９】

図１６に戻って、機密情報サーバ３１は、図６に示す機密情報グループテーブルＴＢ５に基づいて、機密データＳＤＴの暗号化および電子署名の処理を行い（＃２２）、その処理内容を示す処理完了情報ＤＴ１をポリシー管理サーバ２１に送信する（＃２３）。

【００７０】

ポリシー管理サーバ２１は、各営業所の暗号ポリシーの適用状況の集計を行う（＃１２）。集計は、その営業所から受信した処理完了情報ＤＴ１と機密情報グループテーブルＴＢ５（図６参照）および例外属性テーブルＴＢ８（図１０参照）とを比較することによって行う。全営業所についての集計が完了すれば、その結果をディスプレイ装置に表示しまたはレポートとして印刷する。なお、一部の営業所についてのみ集計を行ってもよい。

【００７１】

集計の結果、所定の期間を経過してもなお暗号ポリシーの適用がなされていない場合は（＃１３でＮｏ）、その営業所に対して警告メッセージを送信する（＃

１４）。

【００７２】

警告を受けた営業所の機密情報サーバ３１は、暗号ポリシーが正しく適用されるように、ステップ＃２２、＃２３の処理をやり直す（＃２４でＹｅｓ）。また、必要に応じて、機密情報グループ（図６参照）または利用者グループ（図７参照）などの設定をやり直す（＃２１）。そして、ポリシー管理サーバ２１によって、暗号ポリシーの適用がなされていることが確認されれば（＃１３でＹｅｓ）、その営業所の暗号ポリシーの適用が完了する（＃２４でＮｏ）。

【００７３】

暗号ポリシーの適用が完了した後、ポリシー管理サーバ２１は、図１９に示すように、暗号化に用いられた暗号鍵および電子署名に用いられた署名鍵の有効期限（図５、図８参照）の監視、および暗号方式などの脆弱性の監視を行う（＃３１）。

【００７４】

監視によって暗号鍵または署名鍵の有効期限切れが見つかった場合は、その暗号鍵または署名鍵を使用している営業所に対して、暗号化または電子署名の処理を再度行うように指示する（＃３２）。または、有効期限が切れる所定の期間前に予告するようにしてもよい。

【００７５】

監視によって脆弱性が見つかった場合は、各営業所に対して注意を促す。また、必要に応じて、暗号化または電子署名をやり直すように指示し、そのための支援を行う（＃３２）。つまり、脆弱性に対処した新しい暗号化用データＤＴ５または暗号化ランクテーブルＴＢ４（図５参照）を各機密情報サーバ３１に送信し、これに基づいて暗号化または電子署名のやり直しをさせる。特定の営業所に脆弱性が見つかった場合は、例外属性テーブルＴＢ８に暗号化ランクの例外を設定し、その設定の内容（図１１参照）をその営業所に送信する。

【００７６】

指示または予告を受けた営業所の機密情報サーバ３１は、新しい暗号鍵または署名鍵を生成し、暗号化または電子署名の処理をやり直す（＃４２）。ただし、

新しい暗号化用データＤＴ５、新しい暗号化ランクテーブルＴＢ４、または暗号化ランクの例外を受信した場合は、これらをインストールしてから（＃４１）、ステップ＃４２の処理を行う。暗号化ランクテーブルＴＢ４（図５参照）に変更があった場合は、必要に応じて機密情報グループテーブルＴＢ５（図６参照）の内容を修正し、これに基づいてステップ＃４２の処理を行う。そして、処理が完了した旨をポリシー管理サーバ２１に通知する（＃４３）。

【００７７】

ポリシー管理サーバ２１は、図１６（ａ）のステップ＃１２～＃１４と同様に、暗号ポリシーの適用状況を集計し、正しく適用されていない営業所に対して警告を行う（＃３４でＮｏ、＃３５）。警告を受けた営業所の機密情報サーバ３１は、ステップ＃４１～＃４３の処理をやり直す（＃４４でＹｅｓ）。

【００７８】

暗号化された機密情報の機密データＳＤＴへのアクセス要求があった場合は、機密情報サーバ３１は、図２０に示すように、要求元のユーザ（社員）にアクセス権があるか否かを機密情報グループテーブルＴＢ５（図６参照）に基づいて判別する（＃５１）。

【００７９】

アクセス権がある場合は（＃５１でＹｅｓ）、その機密データＳＤＴを復号し、その社員に対して表示する（＃５２）。機密データＳＤＴの内容が更新された場合は（＃５３）、更新後の機密データＳＤＴに対して暗号化および電子署名の処理を行い（＃５４）、更新があった旨を示すログ情報ＬＤＴをポリシー管理サーバ２１に送信する（＃５５）。アクセス権がない場合は（＃５１でＮｏ）、アクセスの試みがあった旨を示すログ情報ＬＤＴをポリシー管理サーバ２１に送信する（＃５５）。

【００８０】

営業所において機密情報の機密情報グループを変更しまたは社員の配属を変更する場合は、図２１に示すように、図６、図７、または図８の各テーブルを更新する（＃６１）。必要に応じて、暗号化および電子署名の処理をやり直す（＃６２）。そして、更新されたテーブルをポリシー管理サーバ２１に送信する（＃６

３）。

【００８１】

本実施形態によると、システム管理部門が暗号化および電子署名などの情報を一元管理しかつ暗号ポリシーの適用の状況を監視することによって、営業所などの部門ごとに自らの情報を管理しつつ高水準のセキュリティの維持を容易に図ることができる。

【００８２】

また、従来のシステムであれば、外部からの不正なアクセスがあった場合に、その機関で取り扱う情報の内容を改ざんされてしまう可能性があった。その機関に属する職員が情報を改ざんする可能性もないとは言えない。これに対して、本実施形態によると、電子署名の処理を適宜やり直すことによって、従来よりも情報を改ざんしにくくし、機密情報の保護の強化を図ることができる。この場合の処理の実行のタイミングは、暗号化の場合と同様にシステム管理部門が一元管理するので、各営業所にとってシステム管理の負担が軽減される。

【００８３】

本実施形態のセキュリティシステム１をアウトソーシングシステムのために適用することも可能である。例えば、情報管理の支援を行うアウトソーシング会社に暗号化支援システム２を設け、その支援を受けたい者は機密情報サーバ３１を用意すればよい。これにより、小規模企業（いわゆるＳＯＨＯ）や個人にとっても、容易に高度なセキュリティを得ることができる。

【００８４】

その他、セキュリティシステム１、暗号化支援システム２、情報管理システム３、ポリシー管理サーバ２１、機密情報サーバ３１の全体または各部の構成、テーブルの内容、暗号方式、署名方式、処理内容、処理順序などは、本発明の趣旨に沿って適宜変更することができる。

（付記１）情報を管理する情報管理システムと、前記情報管理システムにおいて情報の暗号化を行うための支援を行う暗号化支援システムと、を有し、

前記暗号化支援システムには、

情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示

す規則情報を記憶する暗号化規則記憶手段と、

前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する暗号化用データ送信手段と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理情報受信手段と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、

前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、が設けられ、

前記情報管理システムには、

前記暗号化用データを前記暗号化支援システムより受信する暗号化用データ受信手段と、

当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、

当該情報管理システムが管理する情報の暗号化を、前記暗号化データ受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、

前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、

前記暗号化手段によって行われた暗号化についての前記処理情報を前記暗号化支援システムに送信する処理情報送信手段と、が設けられ、

てなることを特徴とするセキュリティシステム。

（付記２）前記規則情報は、前記規則として、暗号化を行う際に用いる暗号方式と当該暗号化の際に使用する暗号鍵の有効期限とを示し、

前記情報管理システムが情報に暗号化を施した時から現在までの時間が当該情報の区分に対応する前記秘密レベルの前記規則に係る前記有効期限を超えた場合に、

前記警告手段は、当該情報管理システムに対して前記警告を与え、

前記規則情報に示される前記暗号方式が変更された場合に、

前記暗号化用データ送信手段は、当該変更された暗号方式による暗号化を行うための前記暗号化用データを前記情報管理システムに送信し、

前記警告手段は、前記警告として、当該変更された暗号方式に従って情報の暗号化を行うべき旨の警告を与える、

付記１記載のセキュリティシステム。

（付記３）前記情報管理システムには、

当該情報管理システムが管理する情報の区分と当該区分に対応する前記秘密レベルとを示す区分秘密レベル情報を前記暗号化支援システムに送信する区分秘密レベル送信手段が設けられ、

前記監視手段は、情報管理システムより受信した前記処理情報と前記区分秘密レベル情報とを比較することによって前記監視を行う、

付記１または付記２記載のセキュリティシステム。

（付記４）情報に対して電子署名を行うための証明書の有効期限を管理する有効期限管理手段を有し、

前記監視手段は、前記証明書の有効期限に基づいて、情報に対して電子署名をやり直す必要があるか否かを監視し、

前記警告手段は、電子署名をやり直す必要があると判別された場合に、当該情報を管理する前記情報管理システムに対して電子署名をやり直すべき旨の警告を与える、

付記１ないし付記３のいずれかに記載のセキュリティシステム。

（付記５）暗号化支援システムが提供する、情報の暗号化を行うための支援を受けることによって、情報を管理する情報管理システムであって、

情報を秘密にしたいレベルである秘密レベルごとに定められた、情報の暗号化の規則を示す規則情報と、当該規則に従って情報の暗号化を行うために必要なデータである暗号化用データとを、前記暗号化支援システムより受信する受信手段と、

当該情報管理システムが管理する情報の区分を、当該区分ごとに前記秘密レベルと対応付けて記憶する区分別秘密レベル記憶手段と、

当該情報管理システムが管理する情報の暗号化を、前記受信手段によって受信した、当該情報の区分に対応する前記秘密レベルの前記暗号化用データを用いて行う暗号化手段と、

前記暗号化手段によって暗号化が施された情報を記憶する情報記憶手段と、

前記規則に従って情報の暗号化が行われたか否かのチェックを受けるために、前記暗号化手段によって行われた暗号化の処理の内容を示す処理情報を前記暗号化支援システムに送信する処理情報送信手段と、

が設けられてなることを特徴とする情報管理システム。

（付記６）情報を管理する情報管理システムに対して情報の暗号化を行うための支援を行う暗号化支援システムであって、

情報を秘密にしたいレベルである秘密レベルごとに、情報の暗号化の規則を示す規則情報を記憶する暗号化規則記憶手段と、

前記規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する送信手段と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する受信手段と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う監視手段と、

前記監視手段によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える警告手段と、

が設けられてなることを特徴とする暗号化支援システム。

（付記７）セキュリティ情報提供手段より受信した、セキュリティの脆弱性に関する脆弱性情報に基づいて、現在用いられている暗号化の規則の妥当性を監視する妥当性監視手段を有し、

前記送信手段は、現在用いられている暗号化の規則の妥当性がないと判別された場合に、当該規則を適切に変更するための前記暗号化用データを前記情報管理システムに送信する、

付記６記載の暗号化支援システム。

（付記８）情報を管理する情報管理システムに対して情報の暗号化を行うための支援を行うコンピュータに用いられるコンピュータプログラムであって、

情報を秘密にしたいレベルである秘密レベルごとの、情報の暗号化の規則を示す規則情報と当該規則に従って情報の暗号化を行うために必要なデータである暗号化用データを前記情報管理システムに送信する処理と、

前記情報管理システムが行った暗号化の処理の内容を示す処理情報を当該情報管理システムより受信する処理と、

前記情報管理システムにおいて前記規則に従って情報の暗号化が行われているか否かの監視を、当該情報管理システムより受信した前記処理情報に基づいて行う処理と、

前記監視によって見つけられた、前記規則に従って情報の暗号化を行っていない前記情報管理システムに対して、当該規則に従って情報の暗号化を行うべき旨の警告を与える処理と、

をコンピュータに実行させるためのコンピュータプログラム。

【００８５】

【発明の効果】

本発明によると、部門ごとに自らの情報を管理しつつ、高水準のセキュリティの維持を容易に図ることができる。

【図面の簡単な説明】

【図１】

本発明に係るセキュリティシステムの構成の例を示す図である。

【図２】

機密情報サーバのハードウェア構成の例を示す図である。

【図３】

機密情報サーバの機能的構成の例を示す図である。

【図４】

ポリシー管理サーバの機能的構成の例を示す図である。

【図５】

暗号化ランクテーブルの例を示す図である。

【図６】

機密情報グループテーブルの例を示す図である。

【図７】

部署メンバーテーブルの例を示す図である。

【図８】

署名期限テーブルの例を示す図である。

【図９】

作成データ管理テーブルの例を示す図である。

【図１０】

システム管理部門が有する例外属性テーブルの例を示す図である。

【図１１】

ある営業所が有する例外属性テーブルの例を示す図である。

【図１２】

顧客連絡先テーブルの例を示す図である。

【図１３】

検針情報テーブルの例を示す図である。

【図１４】

料金支払テーブルの例を示す図である。

【図１５】

暗号化および電子署名の処理の手順の例を示す図である。

【図１６】

暗号化および電子署名の処理の流れの例を説明するフローチャートである。

【図１７】

システム管理部門側の準備の処理の流れの例を説明するフローチャートである

。

【図１８】

営業所側の準備の処理の流れの例を説明するフローチャートである。

【図１９】

運用開始後の処理の流れの例を説明するフローチャートである。

【図２０】

機密情報へのアクセス要求があった場合の機密情報サーバにおける処理の流れの例を説明するフローチャートである。

【図２１】

各種設定の変更があった場合の機密情報サーバにおける処理の流れの例を説明するフローチャートである。

【符号の説明】

１　セキュリティシステム

２　暗号化支援システム

３　機密情報管理システム（情報管理システム）

２０２　ポリシー情報配付部（暗号化用データ送信手段、送信手段）

２０３　適用状況監視部（処理情報受信手段、監視手段、受信手段）

２０５　適用警告部（警告手段）

２Ｄ１　暗号ポリシーデータベース（暗号化規則記憶手段）

３０２　ポリシー適用部（暗号化用データ受信手段、受信手段）

３０３　暗号化実行部（暗号化手段）

３０４　署名処理実行部（処理情報送信手段）

３０６　グループ情報通知部（区分秘密レベル送信手段）

３Ｄ１　暗号ポリシーデータベース（区分別秘密レベル記憶手段）

３Ｄ２　機密情報グループデータベース（区分別秘密レベル記憶手段）

３Ｄ５　機密情報データベース（情報記憶手段）

ＤＴ１　処理完了情報（処理情報）

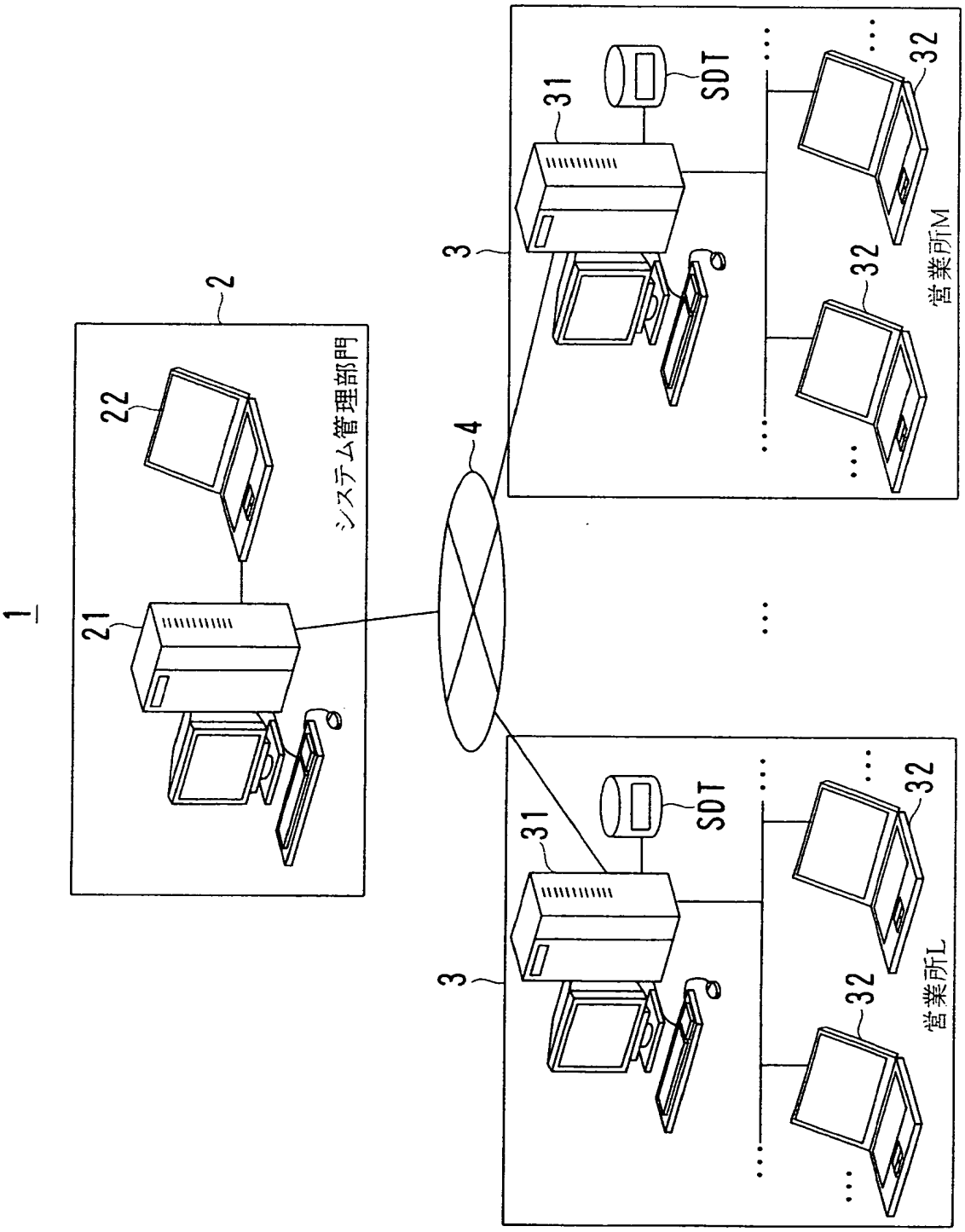
ＤＴ５　暗号化用データ

ＳＤＴ　機密データ

【書類名】　図面

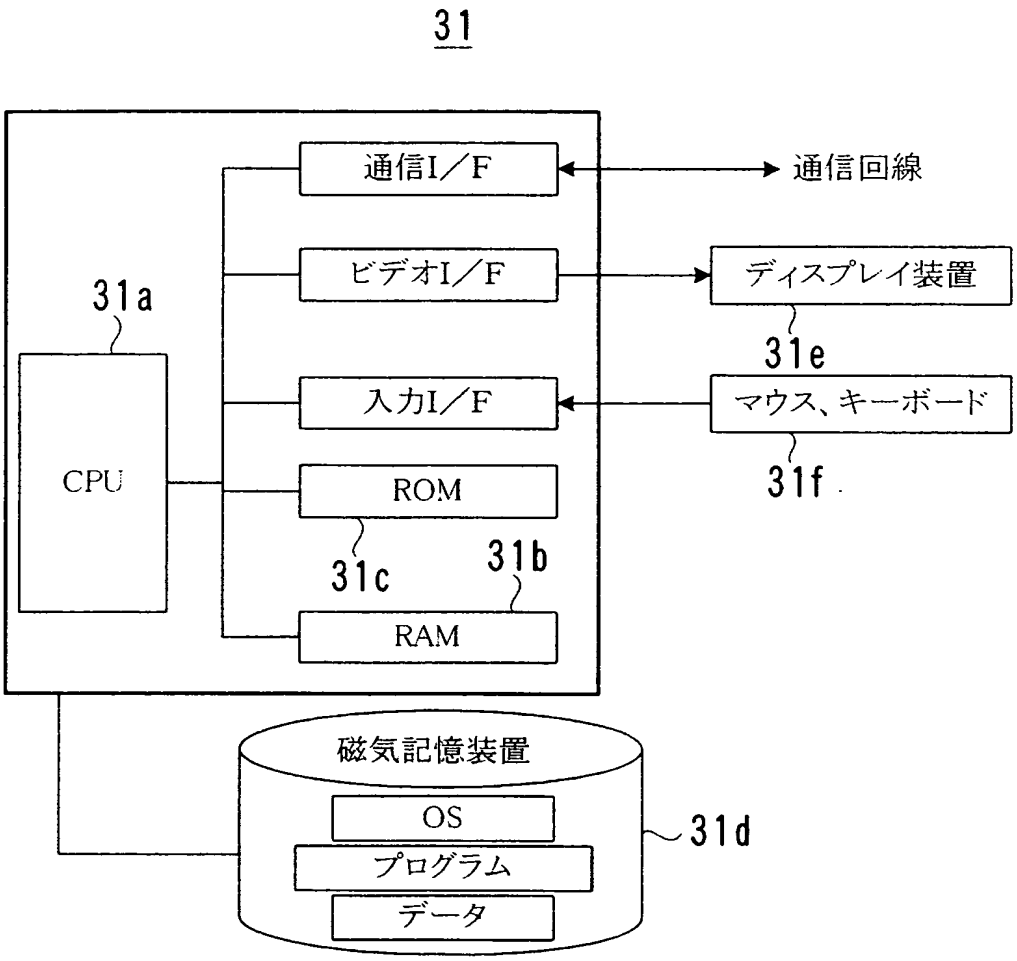
【図１】

本発明に係るセキュリティシステムの構成の例を示す図



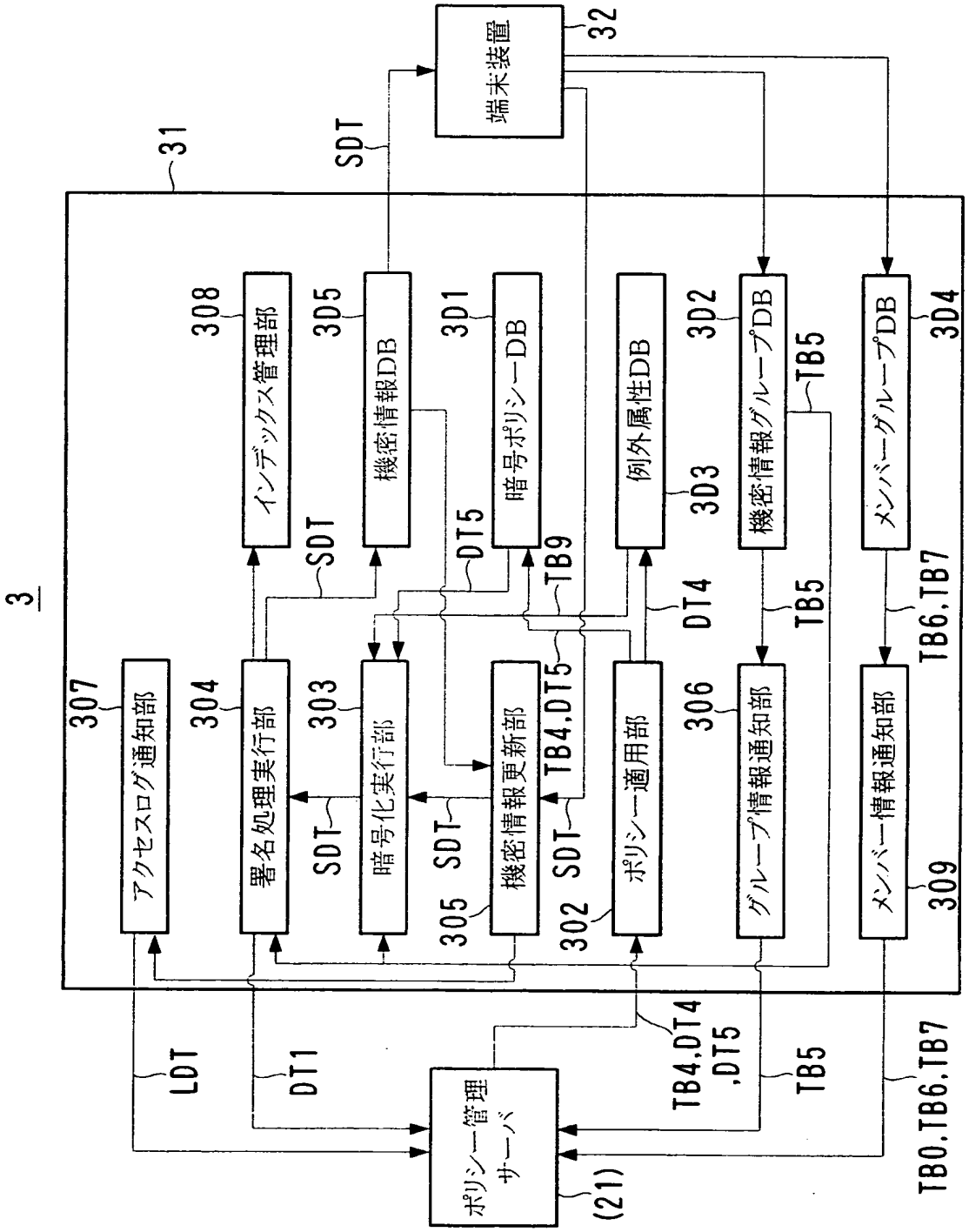
【図２】

機密情報サーバのハードウェア構成の例を示す図



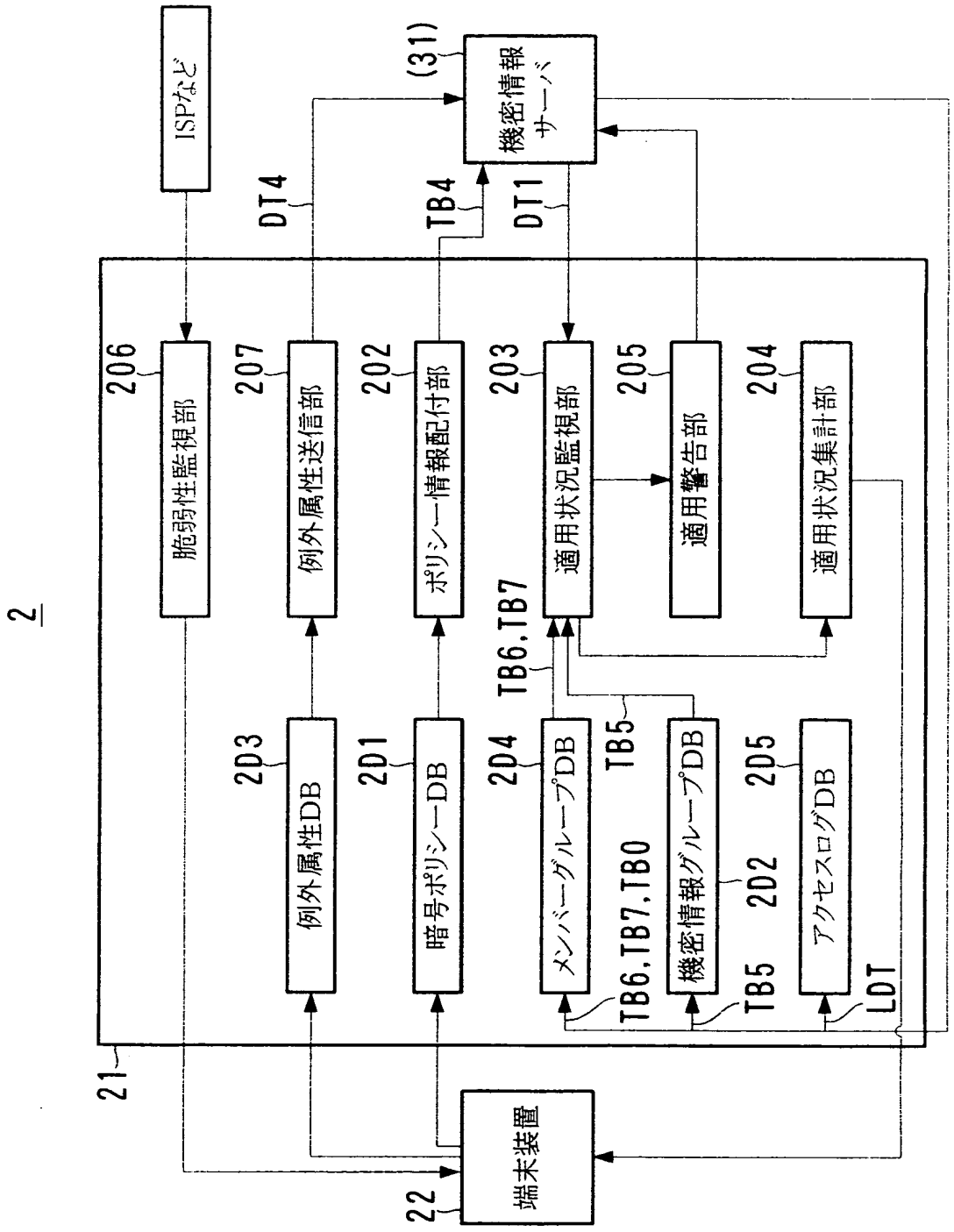
【図３】

機密情報サーバの機能的構成の例を示す図



【図４】

ポリシー管理サーバの機能的構成の例を示す図



【図５】

暗号化ランクテーブルの例を示す図

TB4

暗号化ランク	暗号方式	更新頻度(有効期限)	機密情報(区分)
A	α暗号方式	60日	他社秘密情報(秘密度＝高)
B	β暗号方式	600日	社内人事情報
C	γ暗号方式 or σ暗号方式	無期限	顧客情報
D	β暗号方式	無期限	内線番号一覧情報 他社秘密情報(秘密度＝低)
⋮	⋮	⋮	⋮

【図６】

機密情報グループテーブルの例を示す図

TB5

サーバID	サーバのある営業所	機密情報グループ	暗号化ランク	利用者グループ	機密情報の区分（格納場所）	暗号方式	暗号化ビット数	レコード数
S001	営業所M	G1	C	第1課（顧客窓口）	検針情報テーブル 料金支払いテーブル	σ暗号方式	128bit	100
S001	営業所M	G2	B	第2課（人事課）	社内人事情報テーブル	β暗号方式	256bit	50
S001	営業所M	G3	C	第3課（開発課）	ソースファイルディレクトリ	σ暗号方式	128bit	100
S002	営業所L	G4	A	第4課（営業課）	プレゼン用ディレクトリ	α暗号方式	256bit	25
：	：	：	：	：	：	：	：	：

【図７】

部署メンバーテーブルの例を示す図

TB6

サーバID	利用者グループ（部署）	メンバー1（社員1）	メンバー2（社員2）	・・・
S001	第1課	鈴木 ○朗	山田 △子	・・・
	第2課	田中 ○夫	吉田 △子	・・・
	⋮	⋮	⋮	

【図８】

署名期限テーブルの例を示す図

TB7

サーバID	利用者グループ（部署）	メンバー（社員）	有効期限	署名方式	署名ビット数
S001	第1課	鈴木 ○朗	2005/11/30	RSA	1024bit
	第1課	山田 △子	2006/06/30	RSA	1024bit
	⋮	⋮	⋮	⋮	⋮

【図９】

作成データ管理テーブルの例を示す図

TB0a(TB0)

鈴木　○郎

サーバID	機密情報グループ	文書ID
S001	G1	004
S001	G1	077
S001	G3	200
⋮	⋮	⋮

TB0b(TB0)

山田　△子

サーバID	機密情報グループ	文書ID
S001	G2	076
S001	G3	203
⋮	⋮	⋮

⋮

【図１０】

システム管理部門が有する例外属性テーブルの例を示す図

TB8

営業所(部門)	機密情報の区分	暗号化ランク
営業所M	社内人事情報テーブル	A
営業所L	検針情報テーブル	A
全社	料金支払テーブル	A
⋮	⋮	⋮

【図１１】

ある営業所が有する例外属性テーブルの例を示す図

TB9

機密情報の区分	暗号化ランク	
社内人事情報テーブル	A	～DT4
料金支払テーブル	A	～DT4
⋮	⋮	

【図１２】

顧客連絡先テーブルの例を示す図

TB1

顧客番号	氏名	住所	電話番号	
A0001	○田 一郎	AA県BB市CC町…	012-345-6789	～SDT
A0002	△山 太郎	AA県BB市DD町…	012-345-0000	～SDT
⋮	⋮	⋮	⋮	

【図１３】

検針情報テーブルの例を示す図

TB2

顧客番号	検針値	
A0001	950kWh	～SDT
A0002	815kWh	～SDT
⋮	⋮	

【図１４】

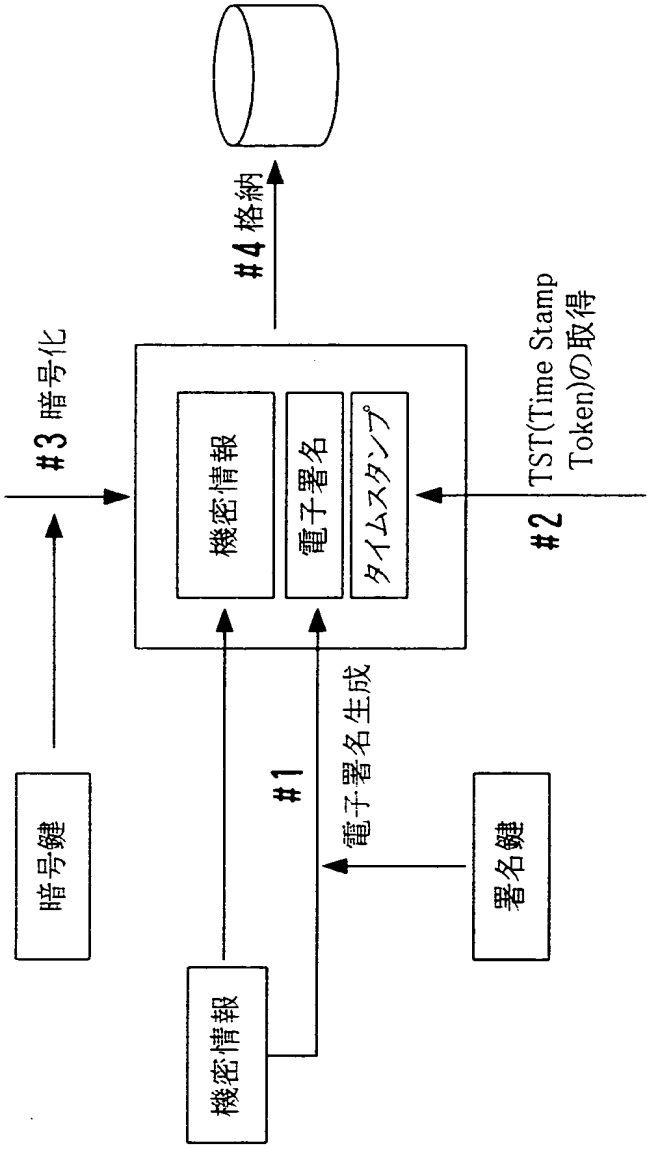
料金支払テーブルの例を示す図

TB3

顧客番号	支払方法	口座番号	
A0001	銀行自動引落し	X銀行Y支店普通012345	～SDT
A0002	窓口支払	－	～SDT
⋮	⋮	⋮	

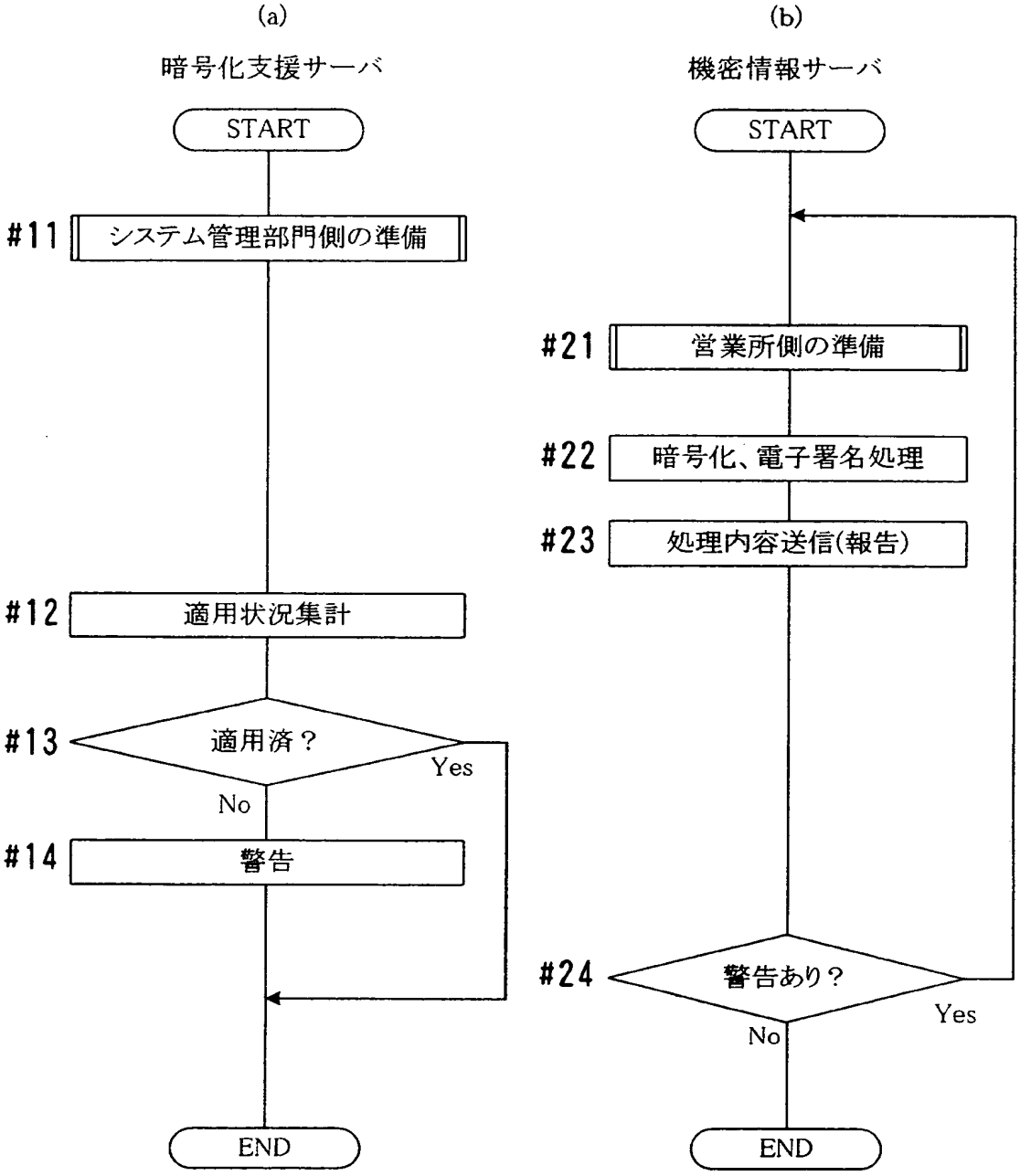
【図１５】

暗号化および電子署名の処理の手順の例を示す図



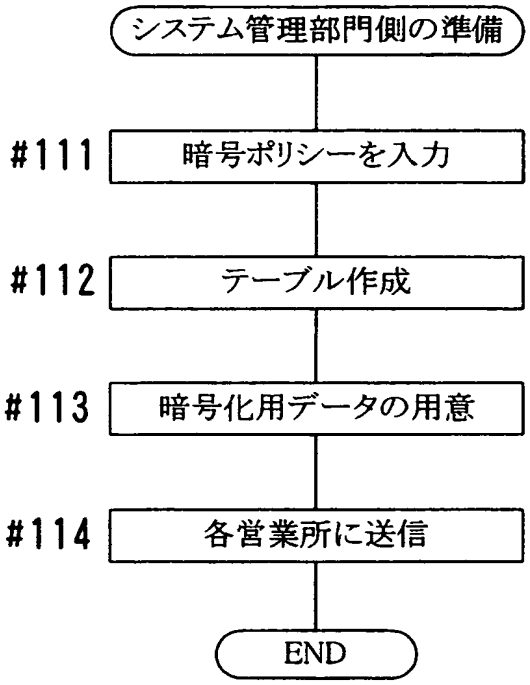
【図１６】

暗号化および電子署名の処理の流れの例を説明するフローチャート



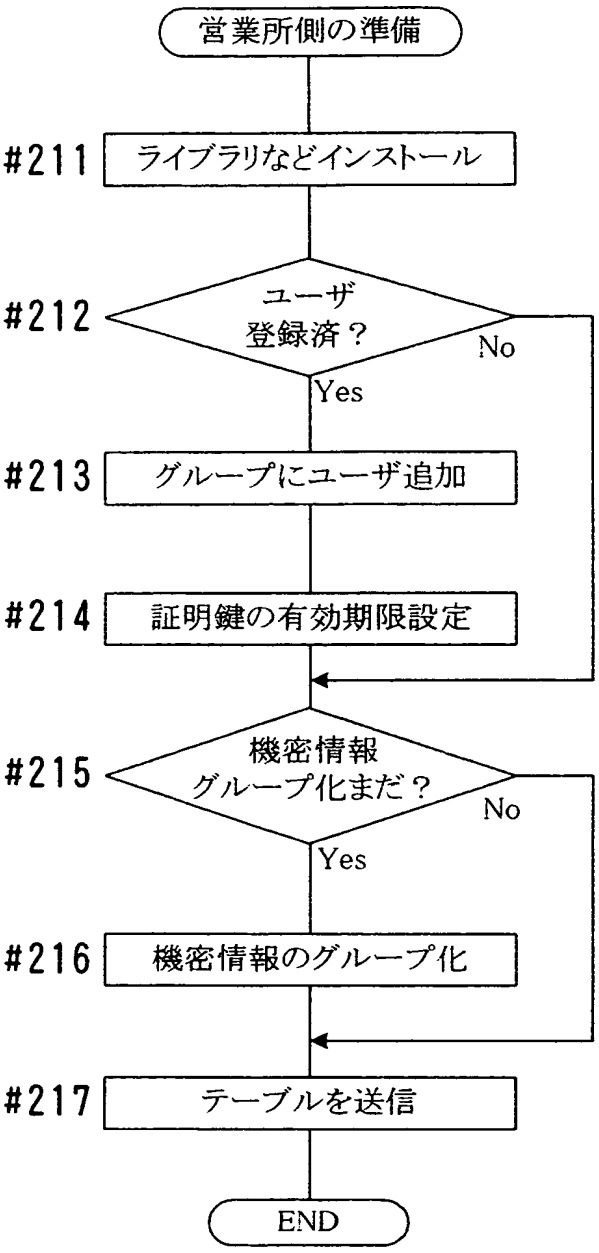
【図１７】

システム管理部門側の準備の処理の流れの例を説明するフローチャート



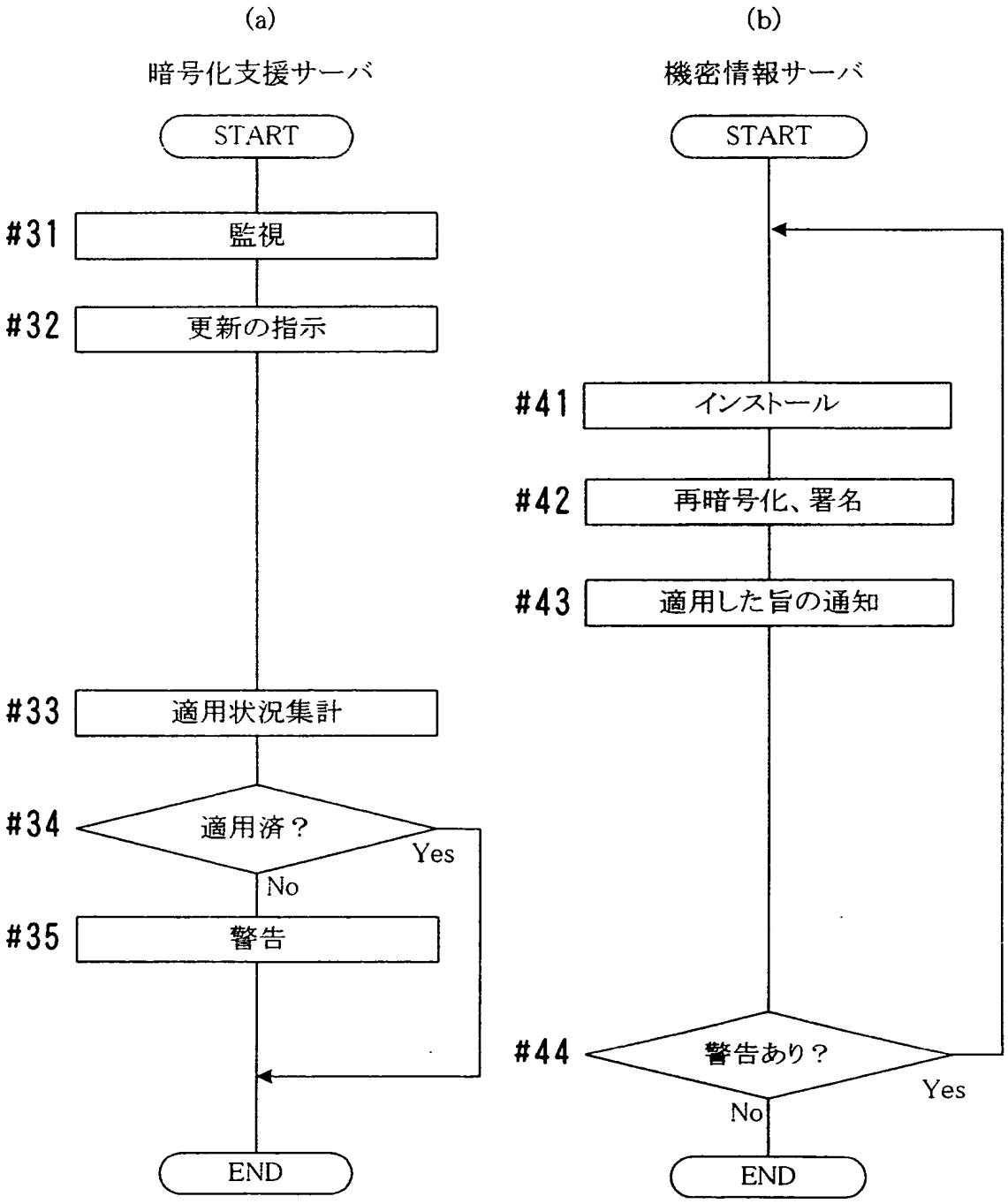
【図１８】

営業所側の準備の処理の流れの例を説明するフローチャート



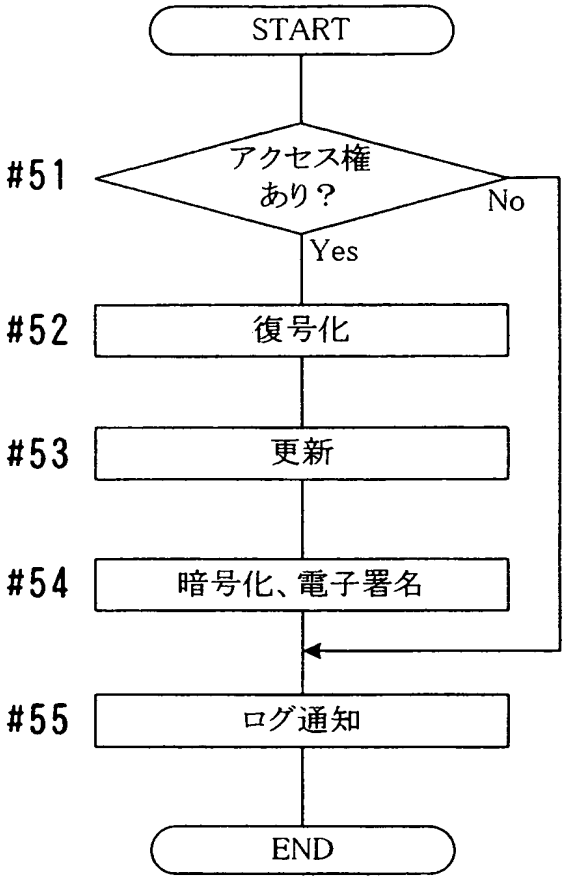
【図１９】

運用開始後の処理の流れの例を説明するフローチャート



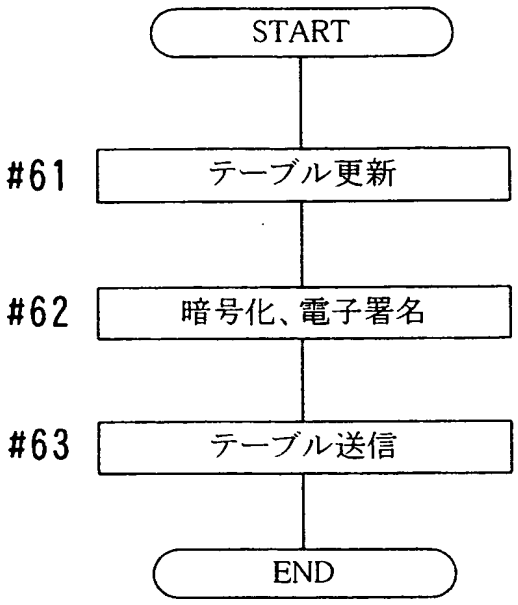
【図２０】

機密情報へのアクセス要求があった場合の機密情報サーバにおける処理の流れの例を説明するフローチャート



【図２１】

各種設定の変更があった場合の機密情報サーバにおける
処理の流れの例を説明するフローチャート



【書類名】　　要約書

【要約】

【課題】部門ごとに自らの情報を管理しつつ、高水準のセキュリティの維持を容易に図る。

【解決手段】暗号化支援システム２は、暗号化の規則を秘密レベルごとに記憶し、規則に従って情報の暗号化を行うために必要な暗号化用データを機密情報管理システム３に送信し、機密情報管理システム３が行った暗号化の処理の内容を示す処理情報を受信し、機密情報管理システム３において規則に従って情報の暗号化が行われているか否かの監視を、その機密情報管理システム３より受信した処理情報に基づいて行い、規則に従って情報の暗号化を行っていない情報管理システム３に対して警告を与える。機密情報管理システム３は、暗号化用データを暗号化支援システム２より受信し、自ら管理する情報の区分を秘密レベルと対応付けて記憶し、自ら管理する情報の暗号化をその情報の区分に対応する秘密レベルの暗号化用データを用いて行い、暗号化が施された情報を記憶し、行った暗号化についての処理情報を暗号化支援システム２に送信する。

【選択図】　　図１

特願２００３－０５１８４２

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社